Claims:

1) Division

5   In any circuit or computer program for computing reciprocals

in a mathematical system such as a finite field or ring or

modular arithmetic system,

where the reciprocal is built up as a linear combination

10   of two or more working variables or registers that are

initialized at the start of the computation,

and where the building up is a sequence of operations

chosen from

shifting a variable,

15   adding one variable to another,

subtracting one variable from another,

negating a variable,

adding or subtracting a multiple of one variable

to or from another,

20   exchanging variables,

permuting variables,

or   renaming variables;

I claim the corresponding method or circuit for computing a

quotient of two quantities, a numerator and a denominator, by

initializing said working variables or registers, at the

start of the computation, to different values, specifically,

5   each working variable or register is initialized to a value

equal to the product of the numerator times the corresponding

initial value from the reciprocal circuit or program.

10   2)   Quadratic Equations.

I claim any circuit or computer program which solves

quadratic equations in a finite field or ring of

characteristic 2 of even degree, by adding, subtracting, or

15   xoring selected values from a table, with the selection being

determined by examining the coefficients and parameters of

the quadratic equation, and quantities derived from the

coefficients and parameters, said values being combined

together with partial solutions determined by directly

20   examining the coefficients and parameters of the equation and

quantities derived from the coefficients and parameters.

3) I claim any method of solving a quadratic equation in a

characteristic 2 field or ring that computes some of the

25   solution bits in a first phase, and then fills in the rest of

the solution bits in subsequent phases.